LINK11

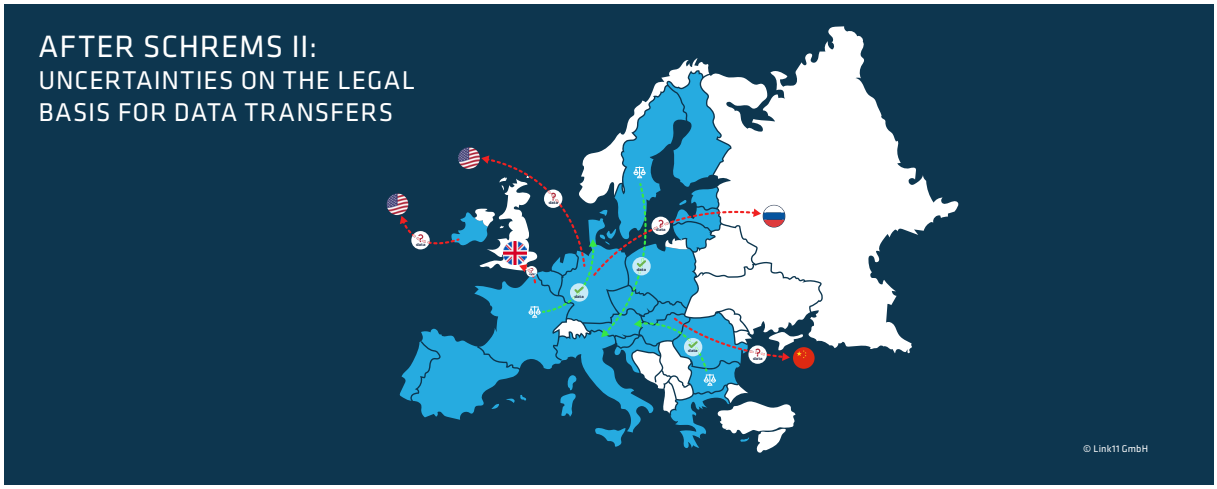
The End of the Privacy Shield for CDN Users

www.link11.com

Following the “Schrems II” ruling by the European Court of Justice, companies should review which data are transferred by their IT solutions.

In its so-called "Schrems II" decision of July 16, 2020, the European Court of Justice ("CJEU") declared the EU-U.S. Privacy Shield invalid. This casts a new light on the trustworthiness of CDN-based IT security solutions from U.S. vendors and, at the same time, brings European providers with high data protection standards to the forefront.

The "Schrems II" ruling is a continuation of the proceedings initiated by the Austrian Maximilian Schrems against Facebook before the Irish High Court with regard to data transfer to the USA In 2015, the CJEU declared the EU's "Safe Harbor" agreement for data transfers to the USA to be invalid. The EU Commission then replaced "Safe Harbor" with the EU-U.S. Privacy Shield. In Schrems II, the CJEU came to the conclusion that the decision of the EU Commission on the EU-U.S. Privacy Shield was invalid. It did not offer a level of protection equivalent to that in the EU, in particular because of extensive state intervention and a lack of legal protection for those affected. The CJEU found the use of standard contractual clauses (SCCs) to be generally sufficient as a legal basis for data transfers outside the EU/EEA. However, it made it clear that in each individual case it had to be examined whether the SCCs were actually complied with in the state of the data recipient. For data transfers to the USA, SCCs are generally not sufficient without additional measures.



With the decision of the European Court of Justice, legal basis for the transatlantic transfer of personal data has been eliminated in many companies. As a result, data transfer to the USA now takes place in a legal grey area. In practice, SCCs are used by most companies for data transfers to non-European countries. Against this background, the Schrems II decision means that companies face great legal uncertainty when using various services such as server hosting, applications for video conferencing, online marketing and web analytics services (i.e., when using cloud-based services).

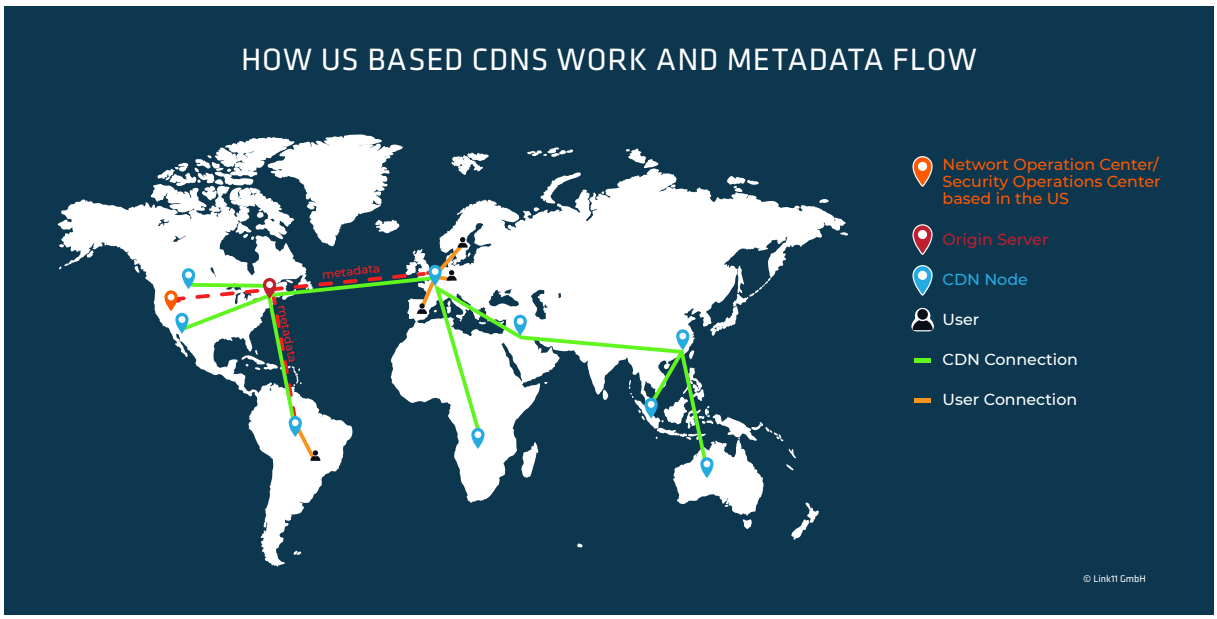
CDN-based protection solutions can also transfer data to the U.S.

U.S. providers of cyber-security services such as DDoS protection or Web Application Firewalls (WAFs) could also be affected by the ruling. Many of these services use a Content Delivery Network (CDN) as a kind of data highway. These CDNs were primarily designed to distribute data (especially media content) around the globe on the Internet via caching. The goal is to shorten the loading times of website content via caches or to deliver web applications securely and quickly at optimum quality. This basically means that requests do not have to be answered by the original server. This helps compensate for load peaks up to a certain level, such as those caused by high-volume DDoS attacks.

CDNs are complex and difficult to adapt tactically to far-reaching regulatory requirements such as those in Schrems II. In a CDN, algorithms are used to control routing and connection optimization; users themselves cannot influence them.

Factors such as latency, packet loss rates, and data throughput are important criteria when it comes to how the data finds its way to the user. Data protection regulations play no role here. In the blink of an eye, data traffic can find itself on overseas cables or outside the EU data protection zone.

What's more, service providers often store log files on U.S. territory and use them within their Network Operation Center (NOC) for the far-reaching optimization of systems in use or to improve the classification of threat situations. Furthermore, the valuable metadata can also be incorporated into the work activities of centrally managed Security Operations Centers (SOCs). They evaluate this to identify threats and fine-tune the relevant filters and protection mechanisms. However, the NOCs and SOCs are all too often located outside the EU – for example in the U.S. The resulting problems were highlighted based on programs such as PRISM and Xkeyscore, which were revealed by Edward Snowden.



In contrast to the CDN-based approach to protecting against DDoS attacks, other security solutions rely on their own protection infrastructure. European providers pursuing this concept are subject to the data protection regulations of their home country, with self-operated filter clusters and networks at all locations. This means they comply with the strict requirements of the GDPR and other national regulations.

Legal recommendations for action

Companies should take direct action to bring international data transfers – to the USA and to countries outside the EU/EEA – in line with the CJEU ruling. The Schrems II ruling affects not only the data transfers into the USA, but its principles are to be considered also for all transfers outside of the EU/EEA.

First of all, responsible companies should take stock and identify any data transfers to third countries, such as the USA. In view of the end of the Brexit transition period on December 31, 2020, transfers to the UK should also be reviewed.

Then the legal basis for international data transfer must be examined. What data is transferred and for what purpose? How are theses data protected in transit and at the destination? Data transfers based on the Privacy Shield should be stopped, provided with additional measures or based on another legal basis.

After the inventory has been made, the risk for the data transfer should be analyzed. What is the legal situation in the third country? Can authorities or government in the destination country access the personal data? Are the rights of the data subjects effectively guaranteed? What technical measures are taken to protect the transferred data? The risk analysis must then be documented.

If SCCs are used as the legal basis for the data transfer, it must be examined are on a case-by-case basis whether the third country offers a level of protection equivalent to that in the EU, e.g., through transparency, technical measures, or legal protection. If the level of protection is not adequate, additional measures must be taken – for instance, (stronger) encryption or anonymization, contractual obligations to observe and to report.

In addition to the SCCs, binding corporate rules or exceptions pursuant to Art. 49 GDPR can also be applied (e.g., consent of the persons concerned).

In addition, it should be considered whether the data can be processed only within the EU/EEA or only in a secure third country. A secure third country is a country outside the EU/EEA for which an EU adequacy decision has been issued. Secure third countries currently include e.g. Andorra, Argentina, Canada (trade organizations only), Israel, Isle of Man, Japan, Jersey, and Switzerland.

With CDNs, for example, it must also be ensured that the transfer of personal data outside the EU/EEA is lawful. The international data transfers must be identified together with their legal basis. The person responsible must perform a risk analysis for the data transfer in each individual case and document the analysis. Then it must be considered what effective legal basis exists for the data transfers and/or where adjustments are necessary.

Personal data in safe hands

Companies that want to play it safe should entrust their data and IT security to a provider from Germany or Europe and thus rule out data transfers to the USA from the outset. The strict regulations of European and German legislators on data protection and data security provide the necessary security for data transmissions. In most cases, this also makes it easier to comply with compliance requirements. To be on the safe side, you should choose a service provider without a branch office in the USA in order to exclude any possible access by the US branch office. An EU provider without US branches offer not only legal aspects but also technical advantages. Moreover, they have a comprehensive and profound knowledge of the European market and the needs of their European customers.

Authors:

Anne Baranowski, LL.M. Attorney at Law, Schalast Rechtsanwälte Notare
Michael Hempe, Regional Sales Director DACH, Link11 GmbH

About Link11

Link11 is the leading European IT security provider in the field of cyber-resilience. The global protection solutions of the Cloud Security Platform are fully automated, react in real-time and defend against all attacks, including unknown and new patterns, in under 10 seconds. According to unanimous analyst opinion (Gartner, Frost & Sullivan) Link11 offers the fastest mitigation (TTM) available on the market. To ensure cyber-resilience, web and infrastructure DDoS protection, bot mitigation, API protection, secure DNS, zero touch WAF, secure CDN, and threat intelligence services, among others, ensure holistic and cross-platform hardening of corporate networks and critical applications. International customers can thus concentrate on their business and digital growth. Since the company was founded in 2005, Link11 has received multiple awards for its innovative solutions.

Link11 GmbH

Lindleystraße 12
60314 Frankfurt
Germany
info@link11.com

Frankfurt Office
+49 (0)69 – 264929777

UK & Ireland Office
+44 (0)203 - 8688711
info.uk@link11.com

Nordics & Baltics Office
+46 (0)85 - 250 05 71
info.nordics@link11.com

BeNeLux Office
+31 (0)68 - 992 3607
info.benelux@link11.com